Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

*Journal of Internet Banking and Commerce, December 2013, vol. 18, no.*3
(*http://www.arraydev.com/commerce/jibc/*)

Strengthening E-Banking security using Keystroke Dynamics

AHMAD KABIR USMAN, MSc
Researcher, Lancashire Business School, University of Central Lancashire, UK
Postal Address: **Lancashire Business School, University of Central Lancashire, Greenbank Building, Preston, Lancashire, PR1 2HE**
Email: ***ausman2@uclan.ac.uk***
Ahmad Usman is a research student at the University of Central Lancashire. His areas of interest are E-Banking Security and Biometric Technologies.

MAHMOOD HUSSAIN SHAH, PhD
Senior Lecturer, Lancashire Business School, University of Central Lancashire, UK
Postal Address: **Lancashire Business School, University of Central Lancashire, Greenbank Building, Preston, Lancashire, PR1 2HE**
Email: ***mhshah@uclan.ac.uk***
Dr. Mahmood Shah is a Senior Lecturer in Business Systems and Cyber Security at the University of Central Lancashire. His research interests are in the areas of cyber security, e-banking, identity theft prevention in e-retailing, e-business and Information Systems.

Abstract

This paper investigates keystroke dynamics and its possible use as a tool to prevent or detect fraud in the banking industry. Given that banks are constantly on the lookout for improved methods to address the menace of fraud, the paper sets out to review keystroke dynamics, its advantages, disadvantages and potential for improving the security of e-banking systems. This paper evaluates keystroke dynamics suitability of use for enhancing security in the banking sector. Results from the literature review found that keystroke dynamics can offer impressive accuracy rates for user identification. Low

costs of deployment and minimal change to users modus operandi make this technology an attractive investment for banks. The paper goes on to argue that although this behavioural biometric may not be suitable as a primary method of authentication, it can be used as a secondary or tertiary method to complement existing authentication systems.

Keywords: **E-Banking; E-banking Frauds Prevention; Internet Banking Security; Fraud Prevention; Keystroke Dynamics, Behavioral Biometric, Biometric Authentication**

INTRODUCTION

With the growing patronage of e-banking services and its anticipated dominance in the near future, some of the known factors capable of hindering its growth must be addressed. The factors that are experienced globally are the increase in security fears, cultural barriers, limited internet access and legislation (Masocha, 2010). For example, in 2010, most of the successful fraud cases were perpetuated via electronic banking systems therefore reflecting weaknesses in the internal control systems (CBN Annual Report, 2010). Therefore more emphasis is required on improving e-banking security systems.

This paper investigates the possibility of strengthening e-banking security using Keystroke Dynamics (KD) as an behavioural biometric authentication system.

Authentication is a critical aspect of e-banking security and new mechanisms for improvement are always being adopted. In Nigeria, the bank regulator reacted to an increase in e-banking fraud by making 2nd level authentication for internet transactions mandatory for all payment cards. This demonstrated the level of importance the Central Bank of Nigeria gives to user authentication and its possible impact on fraud. 'Keystroke Dynamics is the process of analyzing the way users type at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type' (Monrose, 1999). Keystroke Dynamics has drawn attention of researchers due to its relative ease of use and could prove a useful addition to the e-banking security domain.

EXISTING FRAUD PREVENTION TECHNOLOGIES

Today, there are a number of technologies in use to combat fraud in the banking industry. One of these is the use of One Time Passwords (OTPs), which is a fraud prevention technology specific for e-banking transactions. The most basic method displays a time-dependent code that a user is required to input into the banking interface (Johnson 2007). However, such technologies can prove costly to implement costing organisations upto $20 per account holder (Bartholomew 2008). Smart cards and USB tokens are other security measures employed by banks that work by verifying the user

through their possession of a smart card or usb device. The problem is that all existing security measures present one challenge or the other. For example, USB tokens firstly require additional hardware (Council FFIE, 2011), give additional wear and tear on the plug-in interface (Longo and Stapleton, 2002) and are not useful where user permissions are restricted or for devices without USB ports.

Transaction monitoring is a different type of approach that comes from an adaptation of credit/debit card fraud prevention systems. This approach analysis the sender and receiver of the transaction and compares with identified fraud patterns. Any similarity results in the transaction being declined or transferred to a call centre for manual verification. This approach requires no additional hardware for the user as all analysis is done in the background. However, this too comes with its disadvantages, as there will be a loophole in the system when new fraud patterns occur before they are detected. Also, occasionally genuine transactions will be forwarded to call centres which then inconveniences customers.

Two layered passwords is a common fraud prevention measure put in place for authenticating users before providing access to online e-banking services. For authentication to be successful, the user typically needs to know the online banking username and 2 separate passwords. However, the common use of the same password for many services increases the vulnerability of users. Thus, an additional means of security is required for confirming identity. (Moskovitch et al, 2009).

Biometrics for Authentication

Biometric authentication supports the facet of identification, authentication and non-repudiation in information security (Bhattacharyya et al. 2009). Hence, this type of technology can potentially play a pivotal role in minimising e-banking fraud. Biometric technology is seen as a way forward due to the fact that every individual's unique features can be used for identification. Although advances in biometric technologies such as fingerprint, iris recognition and keystroke dynamics appear promising, Murdoch and Anderson (2010) highlighted that secure authentication solutions need to be both technologically sound and economically viable.

Conventional methods of authentication via usernames and passwords are no longer sufficient (Vandommele 2010). Biometric technology is seen as a way forward due to every individual's unique features that can be used for identification. Vandommele (2010) describes the different characteristics of biometrics as Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability and Circumvention. Sarma and Singh (2010) highlight the same characteristics stating that they should be given full consideration when evaluating biometric technology. A comparison of various biometric technologies is given below.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	+	+	+	-	+	-	-
Ear	o	o	+	o	o	+	o
Face	+	-	o	+	-	+	+
Facial thermogram	+	+	-	+	o	+	-
Fingerprint	o	+	+	o	+	o	o
Gait	o	-	-	+	-	+	o
Hand geometry	o	o	o	+	o	o	o
Hand vein	o	o	o	o	o	o	-
Iris	+	+	+	o	+	-	-
Keystroke	-	-	-	o	-	o	o
Odor	+	+	+	-	-	o	-
Palmprint	o	+	+	o	+	o	o
Retina	+	+	o	-	+	-	-
Signature	-	-	-	+	-	+	+
Voice	o	-	-	o	-	+	+

Figure 1 - Comparison of different Biometrics (Vandomele 2010). High, Medium and Low are denoted by +, o, and -

The diagram above provides ratings for biometrics based on 7 characteristics. Bhattacharyya, et al (2009) used False Acceptance Rate (FAR), False Rejection Rate and Equal Error Rate (EER) as factors for evaluating the accuracy of biometric technologies.

Biometric	EER	FAR	FRR	Subjects	Comments
face	NA	1%	10%	37437	varied light, indoor /outdoor
finger print	2%	2%	2%	25000	rotation and exaggerated skin distortion
hand geometry	1%	2%	2%	129	with rings and improper placement
iris	.01%	.94%	.99%	1224	indoor environment
keystrokes	1.8%	7%	.1%	15	during 6 months period
voice	6%	2%	10%	30	text dependent and multilingual

Figure 2 - Evaluation of Biometric Techniques Accuracy (Bhattacharyya et al 2009)

The table above compares research results on biometric techniques with reference to the evaluation factors of biometric technology. The results show that Iris and Face

biometrics are capable of producing the best FAR's while Keystrokes can produce the least FRR's. However the results given above contradict the results from the work of Cho et al (2000) and Lin (1997) where FARs of 0.0% have been achieved. This reflects the improvements in accuracy that researchers have been able to achieve over time.

Research regarding the application of biometric technologies in e-banking exists with the likes of Akinyemi, Omogbadegun, and Oyelami (2011) investigating into how fingerprint technology can be integrated into ATM machines to strengthen the authentication process. The deployment of biometrics to ATM security adds a third layer of security to this e-banking service. Full deployment would certainly reduce the rate of fraudulent activities on ATM machines (Ibidapo et al. 2010). However, this would come at a cost due to the additional hardware required.

KEYSTROKE DYNAMICS FOR IMPROVING BANKING SECURITY

'Keystroke Dynamics is the process of analyzing the way a users type at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type' (Monrose, 1999). Although keystroke dynamics is seen as a relatively a new technology, it was used by the US military to distinguish ally's from the enemy for Morse code messages during World War II (Bartholomew 2008). There has been some research conducted to ascertain its accuracy and suitability for biometric authentication use. More so, a few organisations have also piloted the behavioural biometric seeking to improve their security.

There have been a number of investigations using keystroke dynamics over the years with researchers focusing on improving the levels of accuracy through varying input procedures and algorithms. Lin (1997) experimented with keystroke dynamics using the input of passwords with the length of six to eight characters. This was built on the research conducted by Revett et al (2005) who analysed keystrokes of a passphrase with a constant length of 14 characters for every user. They calculated a similarity measure to create a decision table and used this to determine rules based on rough sets. Revett, Magalhaes and Santos (2005) also carried out a study to identify legitimate and illegitimate login attempts based on the typing style of the user. They found that the typing speed as well as the first few and last characters were the top indicators of whether the login was legitimate or not. An accuracy of 95% was achieved. In some cases, Keystroke Dynamics has already been piloted as a source of improving security as experimented by the work of Foster, Mattoon, and Shearer (2008) cited in Caldarola and MacNeil (2009) for improving security to distance learners during examinations. During this pilot, 100% authentication of all 27 students was achieved. However, keystroke dynamics was used as a secondary security measure rather than primary.

Cho, et al (2000), measured the delay between key presses and the dwell time in order to discriminate between the user and an imposter by using multilayer perceptron neural networks. Neural Networks build a prediction model from historical data, and then uses this model to predict the outcome of a new trial (Shanmugapriya and Padmavathy 2009). Results have shown that using Neural networks for classification achieves better performance than other statistical approaches.

Curtin et al (2006) took a different approach to using Keystroke Dynamics investigating its possible application during long text input scenarios. To carry out their experiments, a custom java application was developed to capture keystroke data. The types of data collated were:

§ Key's Character
§ Key's code text equivalent
§ Key's location on the keyboard (1 = standard, 2 = left, 3= right)
§ Time the key was pressed (milliseconds)
§ Time the key was released (milliseconds)
§ Number of left-mouse click, right-mouse click, and double left-mouse click events during the session

Interestingly the researchers also opted to measure mouse events too and used this as an additional property when creating user signatures. Extractions of the features, averages and standard deviations of key press durations and transition times were used. During the analysis phase, means and standard deviations were calculated. This differs from short text experiments where such analysis is not practicable. Percentages of unique features were also calculated for the style in which users edited text using the various options that a user typically has such as the Insert, delete, backspace and shortcut keys. A total of 50 measurements were used in the experiment. Results were then converted to ranges of 0-1 so that each measurement had the same weight. Classification was then achieved by matching the user with the closest Euclidean distance. Using the Euclidean distance as an analysis method aligns with the discussion by Jamil et al (2011) as one of the analysis methodologies suitable for keystroke dynamics along with weighted and non-weighted probability methodologies.

Results found that up to 100% recognition accuracy could be achieved between 10 users dependant on the entries of text that the Euclidian distance was computed between. The accuracy dropped to 94.7% when the number of users was increased to 30. One of the applications of using such technology was given as being a one of 'n' check (Curtin et al. 2006). From an e-banking perspective, the recognition can assist in investigations where inappropriate actions have been used on a machine to match keystroke data to possible culprits.

Gunetti, et al (2005) experimented keystroke dynamics on free text to enable continuous verification. Bleha et al (1990) took a compromise between the long text input and standard password input by using passphrases for their investigation. Results achieved were an FAR of 0.5% and an FRR of 3.1%. However the algorithm for analysis only covered keystroke latency. It has been found that the best results are achieved when combining both keystroke duration and keystroke latency (Boechat et al. 2006).

.

Surprisingly, mouse dynamics has also proved to have good accuracy with less than 0.5% FAR and 3.29% FRR. However, there is a small caveat as a lengthy 13.55 minutes verification session was required to achieve those results (Fatima 2011). In addition to this, the usage of mice is less common than keyboards, limiting its ability to impact users. However, given the high rate of accuracy, using such a technique may be considered as a complementary measure to use with keystroke dynamics.

Keystroke Dynamics in the Banking Sector

With security experts constantly on the lookout on how improve e-banking security, and keystroke dynamics possessing qualities of a potential good investment, it was only a matter of time before banks adopted such a solution. It has been argued that keystroke dynamics is a more productive and efficient manner for authenticating online systems in comparison with other existing methods (Gunathilake, Padikaraarachchi et al. 2013). Keystroke dynamics based software is a cost effective means of enhancing computer access security (Revett, de Magalhaes et al. 2005a) and therefore makes it also suitable for strengthening internal security of banks as well as online security. Similarly, it has been argued that amongst several biometric approaches, the keystroke dynamics web-based solution is the most relevant due to the low cost of the implementation, satisfactory results as well as the degree of transparency it offers (Choras, Mroczkowski 2007). Unlike many of the other biometric techniques that require high cost capitation devices, keystroke dynamics only requires a keyboard and software (Boechat, Ferreira et al. 2006).

In 2005, the Bank of Ireland considered keystroke dynamics for secondary authentication while others have taken a step further by implementing keystroke dynamics in a bid to improve the security of their e-banking services (Computer Fraud and Security, 2005). Ecuador bank deployed an Authenware solution to measure online behaviour and keystroke patterns. Authenware is commercial software that works by learning and understanding the nuances of a user's keystrokes and behaviours (Authenware 2013). A similar solution has been adopted by the Bank of Utah as they deployed an alternative keystroke dynamic solution; BioPassword, in a bid to make it impossible for anyone other than the authentic users to log into their account (WATCH, 2007). BioPassword is commercially available keystroke dynamics software that uses a neural algorithm to analyze data providing users with a Cross-over Error Rate of 3%. The software has the capability to enrol users immediately, gradual or silently. This therefore highlights how some banks have already invested in keystroke dynamics technology offering their customers an additional level of security.

Challenges in adopting Keystroke Dynamics for Banking Security

Having highlighted the potential of keystroke dynamics and its many advantages, it was left to understand the challenges of adopting such a solution. Vandommele (2010) highlights that keystroke characteristics can change over time and therefore any security system using such a technology will need to have the ability to adapt to this without compromising the security. This is further emphasised by Shanmugapriya and Padmavathy (2009) where they conclude that typing patterns are erratic and can change over time. Given that research in keystroke dynamics is limited, lack of available data sets is a constant challenge as data sets are few in number and are usually small in size (Moskovitch et al. 2009). Banks typically have customers in the range of hundreds of thousands to millions, therefore its accuracy using such large samples of data still needs to be ascertained.

As it stands, little research has been done into the scalability of keystroke dynamics. Therefore the accuracy rates reported from previous research may become unachievable when used by millions of users. Other challenges identified are the cost of storage and the level of administration the system may require (Vandommele 2010). From a banking perspective, banks are familiar in dealing with solutions that have large

storage requirements such as fingerprints or images and would be inclined to invest providing they see the potential value of such a solution. Consequently, it is unlikely that provisioning adequate storage would become a barrier to its adoption.

When it comes to online banking, banks aim to achieve two objectives: convenience and security, and these usually work in friction with each other. Therefore, any solution needs to offer minimal administration to the user ensuring convenience to bank customers. Although Vandomele (2010) highlighted that the level of administration required for keystroke dynamics could become a challenge, Revett, de Magalhaes et al (2005) believe keystroke dynamics is not overly burdensome to the users.

Another substantial challenge with keystroke dynamics is that typing patterns vary based on the type of the keyboard being used, the keyboard layout whether the individual is sitting or standing etc (Shanmugapriya & Padmavathy 2009). In addition to this, there is a level of information required from the onset to be able to create the users signature which goes beyond the usual setup of passwords that users are used to.

With mobile applications growing in popularity, some researchers have turned their attention to user authentication/verification on mobile devices. Studies on mobile devices are minimal which presents opportunity for future work. With banking services now available on mobile devices, the effectiveness of keystroke dynamics on platforms such as IOS, Android etc are yet to be ascertained. Clarke and Furnell (2007) used 11 digit telephone numbers experimenting on text messages and 4 digit PINs to classify users by their keystroke properties. Karnan, Krishnaraj et al (2010) researched into keystroke dynamics on mobile devices attaining 92.8% accuracy, however this was done using a hybrid of keystroke dynamics, fingerprint and palmprint technology. Mobile devices have low computing power therefore will likely prove trickier than personal computers, especially from a performance perspective.

Finally, there are some issues around privacy of users as highlighted by Moskovic (2000). Klonowski, Syga et al. (2012) also placed emphasis on privacy issues and discussed how the use of keystroke dynamics can be exploited for malicious behaviour such as impersonation. Thus, these risks must be adequately mitigated to avoid negative impact.

CONCLUSION

Keystroke dynamics is a lesser-known biometric technology that has potential to authenticate a user with relatively good accuracy. Experiments have proved that accuracy is constantly being improved and software based systems can be as effective as expensive and cumbersome hardware solutions (Revett, de Magalhaes et al. 2005). However, the procedure required for authentication make it unsuitable for use as a primary method of authentication for e-banking security. Nevertheless, the qualities of this behavioural biometric give indication that it will be suitable as a secondary or tertiary security measure for banks. Its ease of implementation, potential low cost of ownership and user-friendliness makes it an ideal candidate for inclusion into the banking security family. Beyond e-banking fraud prevention, this technology has the potential to play a key role in fraud detection by offering investigative features. For example, it can assist in tracing internal fraud in banks by identifying possible culprits even where bank staff may have used shared administrative passwords or their colleague's credentials to access banks systems.

It has been argued that single factor authentication is no longer sufficient and that multi-factor authentication is required to address online banking security cybercrime (Blum 2006). Given the numerous advantages of keystroke dynamics, some banks have already begun using keystroke dynamics for an additional level of security. However, the rate of adoption has been relatively slow. Keystroke dynamic technology can conveniently and efficiently authenticate people (Boechat, Ferreira et al. 2006) making it suitable for improving security across e-banking mediums. Providing that the challenges presented in this paper are addressed, and positive feedback is received from banks that have already introduced the technology into their e-banking security portfolio, we can certainly expect its role in e-banking security to grow.

REFERENCES

Akinyemi, O., Omogbadegun, Z. O., & Oyelami, O. M. (2011). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. arXiv preprint arXiv:1111.7222.

AuthenWare. (2013). http://www.authenware.com/

Bartholomew, D., (2008). The Rhythm Of Identity Management. Baseline, (81), 38-40.

Bartholomew, Doug (2008). "The Rhythm of Identity Management." The Baseline Feb., 38-40

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric Authentication - A Review. International Journal of u- and e- Service, Science and Technology, 2, (3)

BioPassword (2013). http://www.biopassword.com/

Bleha, S., Slivinsky, C., & Hussien, B. (1990). Computer-access security systems using keystroke dynamics. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 12(12), 1217-1222.

Blum, D., (2006). Authentication: Where's The Magic Factor? Network World, 23(16), 51-51.

Boechat, G. C., Ferreira, J. C., & Carvalho, E. C. (2006). Using the keystrokes dynamic for systems of personal security. Transactions on engineering, computing and technology. Enformatika, 18(1), 200-205.

Boechat, G.C., Ferreira, J.C., Carvalho, E.C.B. And Filho, (2006). Using The Keystrokes Dynamic For Systems Of Personal Security. Enformatika, 18, p. 200-205.

Caldarola, R., & MacNeil, T. (2009). Dishonesty Deterrence and Detection: How Technology Can Ensure Distance Learning Test Security and Validity. InProceedings of the 8th European Conference on E-Learning (108-115).

Central Bank of Nigeria, 2012. CBN Annual Report (2010). [online] Available at: <http://www.cenbank.org/Out/2011/publications/reports/rsd/AR2010/Annual%20Report%202010.html> [Accessed 15 January 2012]

Cho, S., Han, C., Han, DH., and Kim, Hi., (2000). Web-Based Keystroke Dynamics Identity Verification Using Neural Network. Journal of Organizational Computing and Electronic Commerce, 10(4):295–307. [Online] Available at: < http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.4863 > [Accessed 20 March 2012]

Choras, M. And Mroczkowski, P., (2007). Web Security Enhancement Based On Keystroke Dynamics, , 01/01 2007, Insticc And Open University Of Catalonia.

Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. International Journal of Information Security, 6(1), 1-14.

Computer Fraud & Security .(2005). Bank Of Ireland Plans To Introduce Two-Factor Authentication, 2005(12), 3-3.

Council, F. F. I. E. (2011). Authentication in an internet banking environment.

Curtin,M., Tappert, C., Villani, M., Ngo, G., Simone, J., Fort, H., and Cha, S., (2006). Keystroke Biometric Recognition on Long-Text Input: A Feasibility Study. [Online] Available at: <http://www.csis.pace.edu/~ctappert/papers/IMECS2006.pdf > [Accessed 7 March 2012]

De Magalhães, S. T., Revett, K., & Santos, H. M. (2005). Password secured sites-stepping forward with keystroke dynamics. In Next Generation Web Services Practices. NWeSP 2005. International Conference on (6-pp). IEEE.

Fatima, A. (2011). E-banking security issues–Is there a solution in biometrics.Journal of

Internet Banking and Commerce [online], 16(2).
Gunathilake, N.M., Padikaraarachchi, A.P.B., Koralagoda, S.P., Jayasundara, M.G., Paliyawadana, P.A.I.M., Manawadu, C.D. And Rajapaksha, U.U.S., (2013). Enhancing The Security Of Online Banking Systems Via Keystroke Dynamics, , 01/01 2013, Ieee Ieee Sri Lanka Sect. Ieee Sri Lanka Sect.
Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. ACM Transactions on Information and System Security (TISSEC), 8(3), 312-347.
Jamil, D., & Khan, M. N. A. (2011). Keystroke Pattern Recognition Preventing Online Fraud. International Journal of Engineering Science and Technology (IJEST), 3(3), 1953-1958.
Karnan, M., Krishnaraj, N., Krishnan, N. And Karthikeyan, M., (2010). Bio Password - Keystroke Dynamic Approach To Secure Mobile Devices, N. Krishnan And M. Karthikeyan, Eds. In: , 01/01 2010, Ieee.
Klonowski, M., Syga, P., Wodo, W., Samarati, P., Lou, W. And Zhou, J., (2012). Some Remarks On Keystroke Dynamics: Global Surveillance, Retrieving Information And Simple Countermeasures, P. Samarati, Wenjing Lou And Jianying Zhou, Eds. In: , 01/01 2012, Insticc Press Insticc Insticc.
Lin, D. T. (1997). Computer-access authentication with neural network based keystroke identity verification. In Neural Networks, 1997., International Conference on (Vol. 1, 174-178). IEEE.Chicago
Longo, E., & Stapleton, J. (2002). PKI Note: Smart Cards. PKI Note Series, PKI Forum.
Masocha, R., Chiliya, N., & Zindiye, S. (2011). E-banking adoption by customers in the rural milieus of South Africa: A case of Alice, Eastern Cape, South Africa. African Journal of Business Management, 5(5), 1857-1863.
Monrose, F., & Rubin, A. (1999). Keystroke dynamics as a biometric for authentication: Future Generation Computer Systems.
Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Lohlein, B., Heister, U., Muler, S., Rokach, L., Elovici, Y., (2009). Identity Theft, Computers and Behavioral Biometrics. [online] Available at: <http://www.ise.bgu.ac.il/faculty/liorr/idth.pdf > [Accessed 6 April 2012]
Murdoch, S. & Anderson, R. (2010), "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication," In Financial Cryptography and Data Security, 6052 ed. R. Sion, ed., Springer Berlin Heidelberg, 336-342.
Revett, K., de Magalhães, S. T., & Santos, H. M. (2005). Enhancing login security through the use of keystroke input dynamics. In Advances in Biometrics (661-667). Springer Berlin Heidelberg.
Revett, K., De Magalhaes, S.T. And Santos, H., (2005). Data Mining A Keystroke Dynamics Based Biometrics Database Using Rough Sets, 01/01 2005, Ieee.
Sarma, G., & Singh, P. K. (2010). Internet banking: Risk analysis and applicability of biometric technology for authentication. International Journal of Pure and Applied Sciences and Technology, 1(2), 67-78.
Shanmugapriya, D., & Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges. arXiv preprint arXiv:0910.0817.
Vandommele, T (2010). Biometric Authentication Today. [Online] Available at: < http://www.cse.hut.fi/en/publications/B/11/papers/vandommele.pdf> [Accessed 15 April 2013]
WATCH, B. (2007). BioPassword secures US $11 m funding after strong 2006.Biometric Technology Today, 5.